CLAIMS

We claim:

1. A printer for outputting content in an encrypted form, the printer comprising:

an interface for receiving the content from an external source;

an encryption module, coupled to the interface to receive the content to be encrypted and to encrypt the content;

a first output system in communication with the encryption module to receive the encrypted content and produce a first output of the encrypted content.

2. The printer of claim 1, wherein the encryption module further comprises:

a metadata generation module for receiving the content to be encrypted and a user selection of a level of security with which decryption information should be outputted, and for generating the decryption information based on the received content and in response to the user selection.

3. The printer of claim 2, further comprising:

a second output system in communication with the metadata generation module to receive the decryption information and to produce a printed output of the decryption information.

4. The printer of claim 2, wherein the decryption information is a key.

5. The printer of claim 2, wherein the decryption information is an identifier of an electronic output of the encrypted content.

6. The printer of claim 2, wherein the decryption information is a description of the content of the encrypted content.

7. The printer of claim 1, wherein the encryption module is further adapted to generate a key and to encrypt the content using the generated key.

8. The printer of claim 1, wherein the encryption module is further adapted to generate a plurality of fractional keys, each fractional key containing a subset of the generated key.

9. The printer of claim 7, wherein the printer further comprises a memory for storing the generated key.

10. The printer of claim 1, wherein the encryption module is further adapted to receive a key, from an external source, and to encrypt the content using the received key.

11. The printer of claim 1, wherein the encryption module is further adapted to decrypt the content.

12. The printer of claim 1, wherein the encryption module is further adapted to encrypt the content using a user private key.

13. The printer of claim 2, wherein the first output system is further adapted to receive generated decryption information and produce an electronic output of the decryption information.

14. The printer of claim 1, wherein the encryption module is further adapted to:

receive, from a source, a public key of an intended recipient,

generate a symmetric key,

encrypt the content with the symmetric key, and

encrypt the symmetric key with the public key.

15. The printer of claim 14, wherein the second output system is further adapted to receive the encrypted symmetric key and to produce a printed output of the encrypted symmetric key.

16. The printer of claim 1, wherein the encryption module is further adapted to generate a plurality of keys, each key is designated to encrypt a corresponding segment of the content.

17. The printer of claim 14, wherein the encryption module is further adapted to receive a plurality of public keys and to encrypt the symmetric key with each received public key.

18. The printer of claim 1, wherein the interface comprises a removable content storage reader.

19. The printer of claim 1, wherein the interface comprises a video input device selected from a group consisting of: a DVD reader, a video cassette tape reader, and a flash card reader.

20. The printer of claim 1, wherein the interface comprises an audio input device selected from a group consisting of: a CD reader, an audio cassette tape reader, and a flash card reader.

21. The printer of claim 1, wherein the interface comprises an embedded receiver selected from a group consisting of: an embedded TV receiver, an embedded radio receiver, an embedded short-wave radio receiver, an embedded satellite radio receiver, an embedded two-way radio, and an embedded cellular phone.

22. The printer of claim 1, wherein the interface comprises an embedded video recorder, wherein the external source of content is a series of images captured by embedded the video recorder, converted into an electrical format, and then provided to the content processing system.

23. The printer of claim 1, wherein the interface comprises an embedded audio recorder, wherein the external source of content is a series of sounds that are converted into an electrical format by the embedded audio recorder and then provided to the content processing system.

24. The printer of claim 1, wherein the first output system is configured to write the electronic representation to a removable media storage device.

25. The printer of claim 24, wherein the removable storage device is selected from a group consisting of: a DVD, a video cassette tape, a CD, an audio cassette tape, a flash card, a computer disk, an SD disk, and a computer-readable medium.

26. The printer of claim 1, wherein the first output system comprises a media writer.

27. The printer of claim 1, wherein the first output system comprises an embedded web page display.

28. A method for outputting encrypted content, the method comprising:

receiving unencrypted content from a source;

encrypting the content, by a printer, to generate a first output of the encrypted content; and

producing the first output of the encrypted content.

29. The method of claim 28, further comprising:

generating a key used to decrypt the content; and

encrypting the content, using the generated key.

30. The method of claim 29, further comprising a step of generating a plurality of fractional keys, each fractional key containing a subset of the generated key.

31. The method of claim 29, further comprising a step of decrypting the encrypted content using the generated key.

32. The method of claim 28, further comprising:

receiving a user's private key; and

encrypting the content using the private key.

33. The method of claim 28, further comprising:

receiving a user selection of a level of security with which decryption information should be outputted;

generating a decryption information, based on the unencrypted content and in response to the user selection; and

producing a second output of the decryption information.

34. The method of claim 28, wherein the source comprises one selected from the group consisting of:

a scanner;

a video device;

an audio device;

a memory card;

a storage device;

a facsimile source;

an email source; and

a wireless source.

35. The method of claim 28, wherein producing the first output further comprises producing an electronic output.

36. The method of claim 28, wherein producing the first output further comprises producing a paper output.

37. The method of claim 33, wherein producing the second output further comprises producing an electronic output.

38. The method of claim 33, wherein producing the second output further comprises producing a paper output.

39. The method of claim 33, wherein the decryption information is an identifier of the first output of the encrypted content.

40. The method of claim 33, wherein the decryption information is a description of the content of the encrypted content.

41. The method of claim 33, wherein the decryption information is a key used to decrypt the encrypted content.

42. The method of claim 28, further comprising:

receiving, from a source, a public key of an intended recipient;

generating a symmetric key;

encrypting the content with the symmetric key; and

encrypting the symmetric key with the public key.

43. The method of claim 28, further comprising:

receiving a plurality of public keys; and

encrypting the symmetric key with each received public key.

44. The method of claim 29, further comprising generating a plurality of keys used to decrypt the content, each generated key is designated to decrypt a corresponding segment of the content.

45. A computer program product comprising a computer-readable medium containing computer program code for performing any one of the methods of claims 28 through 44.